AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. – 26. (Cancelled)

27. (Previously Presented) A method for managing access to a plurality of applications using a central server, comprising:

receiving a user name and a user password of a user from a first application;

authenticating the user using the user name and password;

generating, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user;

generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information;

sending the first artifact to the first application;

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verifying the validity of the first artifact upon receipt from the second application;

retrieving, after successful validation of the first artifact, the identity assertion information for the user using the first artifact;

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application;

rendering the first artifact invalid for future use by any of the plurality of applications;

receiving a request for a second artifact from the second application; and

providing the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information,

wherein the first application and the second application are members of the plurality of applications.

28. (Previously Presented) The method of claim 27, further comprising:

receiving the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verifying the validity of the second artifact upon receipt from the third application;

retrieving, upon successful validation, the identity assertion information for the user using the second artifact;

sending the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application;

rendering the second artifact invalid for future use by any of the plurality of applications;

receiving a request for a third artifact from the second application; and

providing the third artifact associated with the identity assertion information, wherein the third artifact is used to obtain the identity assertion information,

wherein the third application is a member of the plurality of applications.

29. (Previously Presented) The method of claim 27, wherein the identity assertion information is stored in the central server.

30. (Previously Presented) The method of claim 27, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

31. (Previously Presented) The method of claim 30, wherein the first artifact further comprises a server identification.

32. (Previously Presented) The method of claim 27, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

33. (Previously Presented) The method of claim 27, wherein the user name and the user password are obtained by the first application from a web browser.

34. (Currently Amended) A system for managing access to a plurality of applications comprising:

a processor; and

an identity service provider executing on the processor, configured to:

receive a user name and a user password of a user from a first application;

authenticate the user using the user name and password;

generate, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user;

generate a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information;

send the first artifact to the first application;

receive the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verify the validity of the first artifact upon receipt from the second application;

~~retrieving~~ retrieve, after successful validation of the first artifact, the identity assertion information for the user using the first artifact;

send the identity assertion information ~~and the second artifact~~ to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application;

render the first artifact invalid for future use by any of the plurality of applications;

receive a request for a second artifact from the second application; and

provide the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information,

wherein the first application and the second application are members of the plurality of applications.

35. (Previously Presented) The system of claim 34, wherein the identity service provided is further configured to:

receive the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verify the validity of the second artifact upon receipt from the third application;

retrieve, upon successful validation, the identity assertion information for the user using the second artifact;

render the second artifact invalid for future use by any of the plurality of applications;

receive a request for a third artifact from the second application; and

provide the third artifact associated with the identity assertion information, wherein the third artifact is used to obtain the identity assertion information,

wherein the third application is a member of the plurality of applications.

36. (Previously Presented) The system of claim 34, wherein the identity assertion information is stored in the identity service provider.

37. (Previously Presented) The system of claim 34, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

38. (Previously Presented) The system of claim 37, wherein the first artifact further comprises a server identification.

39. (Previously Presented) The system of claim 34, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

40. (Previously Presented) The system of claim 34, wherein the user name and the user password are obtained by the first application from a web browser.

41. (Previously Presented) A computer readable memory comprising program instructions that, when executed by a processor, implement a method managing access to a plurality of applications using a central server, the method comprising:

receiving a user name and a user password of a user from a first application;

authenticating the user using the user name and password;

generating, in response to the successful authentication, identity assertion information comprising information associated with the user for use by a plurality of applications to authenticate the user;

generating a first artifact associated with the identity assertion information, wherein the first artifact is used to obtain the identity assertion information;

sending the first artifact to the first application;

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verifying the validity of the first artifact upon receipt from the second application;

retrieving, after successful validation of the first artifact, the identity assertion information for the user using the first artifact;

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application;

rendering the first artifact invalid for future use by any of the plurality of applications;

receiving a request for a second artifact from the second application; and

providing the second artifact associated with the identity assertion information, wherein the second artifact is used to obtain the identity assertion information,

wherein the first application and the second application are members of the plurality of applications

42. (Previously Presented) The computer readable memory of claim 41, where the method further comprises:

receiving the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verifying the validity of the second artifact upon receipt from the third application;

retrieving, upon successful validation, the identity assertion information for the user using the second artifact;

sending the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application;

rendering the second artifact invalid for future use by any of the plurality of applications;

receiving a request for a third artifact from the second application; and

providing the third artifact associated with the identity assertion information, wherein the third artifact is used to obtain the identity assertion information,

wherein the third application is a member of the plurality of applications.

43. (Previously Presented) The computer readable memory of claim 41, wherein the identity assertion information is stored in the central server.

44. (Previously Presented) The computer readable memory of claim 41, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

45. (Previously Presented) The computer readable memory of claim 44, wherein the first artifact further comprises a server identification.

46. (Previously Presented) The computer readable memory of claim 41, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

47. (Previously Presented) The computer readable memory of claim 41, wherein the user name and the user password are obtained by the first application from a web browser.